(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月11 日 (11.08.2005)

PCT

(10) 国際公開番号
WO 2005/073842 A1

(51) 国際特許分類[7]: G06F 7/58, H03K 3/84

(21) 国際出願番号: PCT/JP2005/001211

(22) 国際出願日: 2005 年1 月28 日 (28.01.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-023335 2004 年1 月30 日 (30.01.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本ビクター株式会社 (VICTOR COMPANY OF JAPAN, LIMITED) [JP/JP]; 〒2218528 神奈川県横浜市神奈川区守屋町３丁目１２番地 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 猪羽 渉 (INOHA, Wataru). 日暮 誠司 (HIGURASHI, Seiji).

(74) 代理人: 三好 秀和 (MIYOSHI, Hidekazu); 〒1050001 東京都港区虎ノ門１丁目２番８号 虎ノ門琴平タワー Tokyo (JP).

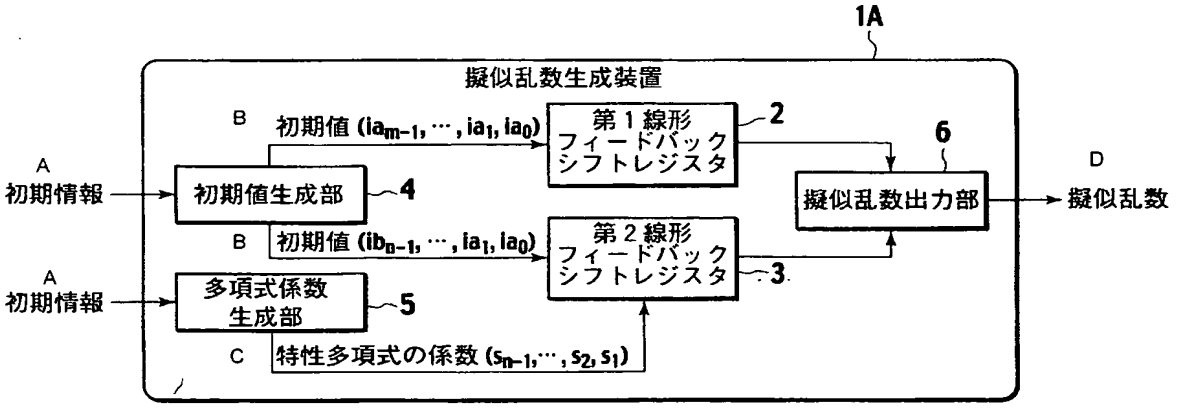
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,

[続葉有]

(54) Title: PSEUDO RANDOM NUMBER GENERATION DEVICE AND PSEUDO RANDOM NUMBER GENERATION PROGRAM

(54) 発明の名称: 擬似乱数生成装置および擬似乱数生成プログラム



A... INITIAL INFORMATION
1A... PSEUDO RANDOM NUMBER GENERATION DEVICE
B... INITIAL VALUE
4... INITIAL VALUE GENERATION UNIT
5... POLYNOMIAL COEFFICIENT GENERATION UNIT
C... CHARACTERISTIC POLYNOMIAL COEFFICIENT
2... FIRST LINEAR FEEDBACK SHIFT REGISTER
3... SECOND LINEAR FEEDBACK SHIFT REGISTER
6... PSEUDO RANDOM NUMBER OUTPUT UNIT
D... PSEUDO RANDOM NUMBER

(57) Abstract: A pseudo random number generation device (1) includes a first linear feedback shift register (2), a second linear feedback shift register (3), an initial value generation unit (4), a polynomial coefficient generation unit (5), and a pseudo random number output unit (6). The initial value generation unit (4) generates an initial value and supplies it to the first linear feedback shift register (2) and the second linear feedback shift register (3). The polynomial coefficient generation unit (5) generates a characteristic polynomial coefficient and supplies it to the second feedback shift register (3). The pseudo random number output unit (6) generates a pseudo random number from the exclusive OR of each bit according to the bit string successively output from the first linear feedback shift register (2) and the second linear feedback shift register (3) and outputs it.

[続葉有]

WO 2005/073842 A1

IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:
— 国際調査報告書

(57) 要約: 擬似乱数生成装置（１）は、第１線形フィードバックシフトレジスタ（２）、第２線形フィードバックシフトレジスタ（３）、初期値生成部（４）、多項式係数生成部（５）および擬似乱数出力部（６）を有する。初期値生成部（４）は、初期値を生成し、第１線形フィードバックシフトレジスタ（２）および第２線形フィードバックシフトレジスタ（３）へ供給する。多項式係数生成部（５）は、特性多項式の係数を生成して第２線形フィードバックシフトレジスタ（３）へ供給する。擬似乱数出力部（６）は、第１線形フィードバックシフトレジスタ（２）および第２線形フィードバックシフトレジスタ（３）から順次出力されるビット列を基に、各ビットの排他的論理和から擬似乱数列を生成、出力する。